Cyber Testing for Resilient Industrial Control Systems (CyTRICS)

The Department of Energy's program for cybersecurity vulnerability testing and digital subcomponent enumeration.

CyTRICS partners across stakeholders to identify high priority operational technology (OT) components, perform expert testing, share information about vulnerabilities in the digital supply chain, and inform improvements in component design and manufacturing.

CyTRICS leverages best-in-class test facilities and analytic capabilities at four DOE National Laboratories and strategic partnerships with key stakeholders including technology developers, manufacturers, asset owners and operators, and interagency partners.

The CyTRICS program comprises several innovative components:

Prioritization Methodology. An approach to prioritizing OT components for testing that incorporates key factors including operational impact, prevalence, and national security interest. This approach provides a strategic, transparent rationale for testing components that optimizes security impact.

Standardized Testing Process. DOE has developed and refined a standardized approach to enumerating and vulnerability testing firmware and software subcomponents. Standardization ensures consistency, repeatability, and comparability of results, to scale up testing and automation across Labs and partners.

Standardized Reporting and Repository. CyTRICS captures testing results in a standard, bill of materials format that captures granular "digital ingredients" to the subcomponent level, to rapidly identify embedded high-risk components and subcomponents. The program features a central repository of testing results for comprehensive, sector-wide analysis of systemic risks and vulnerabilities.

Vendor Agreements. CyTRICS partners with top manufacturers and utilities in the sector to sign participation Agreements to frame mutual cooperation prior to conducting testing. The standard agreement establishes types of software and firmware testing to be performed, timely disclosure of vulnerabilities identified during testing, and coordinated disclosure of vulnerability information with impacted asset owners, federal agencies, and energy sector stakeholders.

CyTRICS completed proof-of-concept testing in 2018. Using the results from that testing, the program developed a draft test operations methodology, results reporting formats, and a repository for findings in 2019. CyTRICS completed a full pilot test of program processes in the fall of 2020.

In 2021, CyTRICS moved into initial operating capability and is scaling up. CESER has engaged industry participants for feedback on key CyTRICS processes including test operations, reporting formats, advanced analytics and risk calculation, and the coordinated vulnerability disclosure process. CESER is continuously refining CyTRICS program processes to reflect industry best practices and evolving policy.

CyTRICS cyber vulnerability testing supports supply chain security needs across multiple DOE initiatives. CESER collects requirements for digital component testing from many programs, sub-sectors, and agencies for inclusion in the CyTRICS testing prioritization methodology.

CyTRICS leverages CESER's Energy Sector engagement forums to ensure transparency and coordination with industry partners. The Securing Energy Infrastructure Executive Task Force, mandated in Section 5726 of the FY2020 National Defense Authorization Act, serves as the primary venue for strategic and technical engagement for energy sector manufacturers, asset owners, and stakeholders in the design and operation of CyTRICS.